K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

April – May 2023
(B.Tech) Program: B. Tech Computer Engineering Scheme: II
Examination: TY Semester: VI
Course Code: CEC602 Course Name: Cryptography and System Security

Date of Exam: 15/05/2023 Duration: 2.5 Hours Max. Marks: 60

Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.

		Max. Marks	CO	BT level
Q 1	**Solve any six questions out of eight:**	**12**		
i)	Find Multiplicative Inverse of 3 MOD 5 using extended euclidean method.	2	CO1	Ap
ii)	Explain CBC Mode of Block Ciphers.	2	CO2	U
iii)	Draw a neat labeled Structure of X.509 standard used for digital certificates.	2	CO2	Ap
iv)	Define cryptographic hash Function and list its properties.	2	CO3	U
v)	What are the drawbacks of password based authentication?	2	CO4	U
vi)	What is meant by Ports and Port scanning?	2	CO5	U
vii)	What are the different vulnerabilities present with the TCP/IP protocol suite?	2	CO5	U
viii)	What is Buffer Overflow Attack?	2	CO6	U
Q.2	**Solve any four questions out of six.**	**16**		
i)	Apply Hill Cipher technique on plaintext "KJS CQMPUTERS" with following key matrix $\begin{vmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 12 & 7 \end{vmatrix}$	4	CO1	Ap
ii)	A RSA cryptosystem uses two prime numbers 3 and 13 to generate the public key= 3 and the private key = 7. What is the value of cipher text for a plain text "e"?	4	CO2	Ap

K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

April – May 2023
(B.Tech) Program: B. Tech Computer Engineering Scheme: II
Examination: TY Semester: VI
Course Code: CEC602 Course Name: Cryptography and System Security

Date of Exam: 15/05/2023 Duration: 2.5 Hours Max. Marks: 60

iii)	Write a Short note on SHA-1 Algorithm.	4	CO3	U
iv)	Write a short note on RSA Digital Signature Standard	4	CO4	U
v)	Explain SYN Flood Attack.	4	CO5	U
vi)	Explain the stages and types of Viruses.	4	CO6	U
Q.3	**Solve any two questions out of three.**	**16**		
i)	Compare Symmetric and Asymmetric Cipher Techniques and apply playfair cipher on following plaintext. "CSS IS MY FAVORITE SUBJECT" using the Key PROFESSOR.	8	CO1	Ap
ii)	What is challenge and response based authentication? Explain all schemes used within it.	8	CO4	U
iii)	What is the difference between DOS and DDOS attacks? Explain any three types of DOS attacks and their countermeasures.	8	CO5	An
Q.4	**Solve any two questions out of three.**	**16**		
i)	With a Suitable diagram explain the detailed working of Kerberos Authentication protocol.	8	CO2	U
ii)	With suitable diagrams explain the working of MD5 algorithm.	8	CO3	U
iii)	Write a note on 1) SQL injection Attack. 2) Firewalls	8	CO6	U

****